

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division**

VOLTAGE HOLDINGS, LLC,
MILLENNIUM FUNDING, INC., SCREEN
MEDIA VENTURES, LLC, DALLAS
BUYERS CLUB, LLC, WONDER ONE,
LLC, MILLENNIUM IP, INC., I AM
WRATH PRODUCTIONS, INC., AMBI
DISTRIBUTION CORP., KILLING LINK
DISTRIBUTION, LLC, BADHOUSE
STUDIOS, LLC, LF2 PRODUCTIONS,
INC., LHF PRODUCTIONS, INC.,
LAUNDRY FILMS, INC., VENICE PI,
LLC, RAMBO V PRODUCTIONS, INC.,
NIKOLA PRODUCTIONS, INC.,
BODYGUARD PRODUCTIONS, INC.,
OUTPOST PRODUCTIONS, INC., and
AFTER II MOVIE, LLC,

Plaintiffs,

v.

DATACAMP LIMITED, a United Kingdom
limited company, and DOES 1-10,

Defendants.

Civil Action No. 1:21-cv-1102

JURY TRIAL DEMANDED

COMPLAINT

VOLTAGE HOLDINGS, LLC, MILLENNIUM FUNDING, INC., SCREEN MEDIA VENTURES, LLC, DALLAS BUYERS CLUB, LLC, WONDER ONE, LLC, MILLENNIUM IP, INC., I AM WRATH PRODUCTIONS, INC., AMBI DISTRIBUTION CORP., KILLING LINK DISTRIBUTION, LLC, BADHOUSE STUDIOS, LLC, LF2 PRODUCTIONS, INC., LHF PRODUCTIONS, INC., LAUNDRY FILMS, INC., VENICE PI, LLC, RAMBO V PRODUCTIONS, INC., NIKOLA PRODUCTIONS, INC., BODYGUARD PRODUCTIONS, INC., OUTPOST PRODUCTIONS, INC. and AFTER II MOVIE, LLC (“Plaintiffs”), by and

through their counsel, bring this Complaint against DATACAMP LIMITED and DOES 1-10 (“Defendants”) and allege as follows:

I. NATURE OF THE ACTION

1. Plaintiffs bring this action under the United States Copyright Act of 1976, as amended, 17 U.S.C. §§ 101, *et seq.* (the “Copyright Act”), and allege that Defendants DOES 1-10 are liable for direct infringements in violation of 17 U.S.C. §§ 106 and 501 and violations under the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 1202.

2. Plaintiffs further allege that Defendants DATACAMP LIMITED (“DataCamp”) and DOES 1-10 are secondarily liable for direct infringements in violation of 17 U.S.C. §§ 106 and 501, secondarily liable for violations under DMCA, 17 U.S.C. § 1202, and liable for injunctive relief pursuant to 17 U.S.C. §§ 512(j).

II. JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over this action pursuant to 17 U.S.C. §§ 101, *et seq.*, (the Copyright Act), 28 U.S.C. § 1331 (federal question), 28 U.S.C. § 1338 (patents, copyrights, trademarks, and unfair competition), and 28 U.S.C. § 1367 (supplemental jurisdiction).

4. Defendants solicit, transact, or are doing business within this jurisdiction, and have committed unlawful and tortious acts both within and outside this jurisdiction with the full knowledge that their acts would cause injury in this jurisdiction.

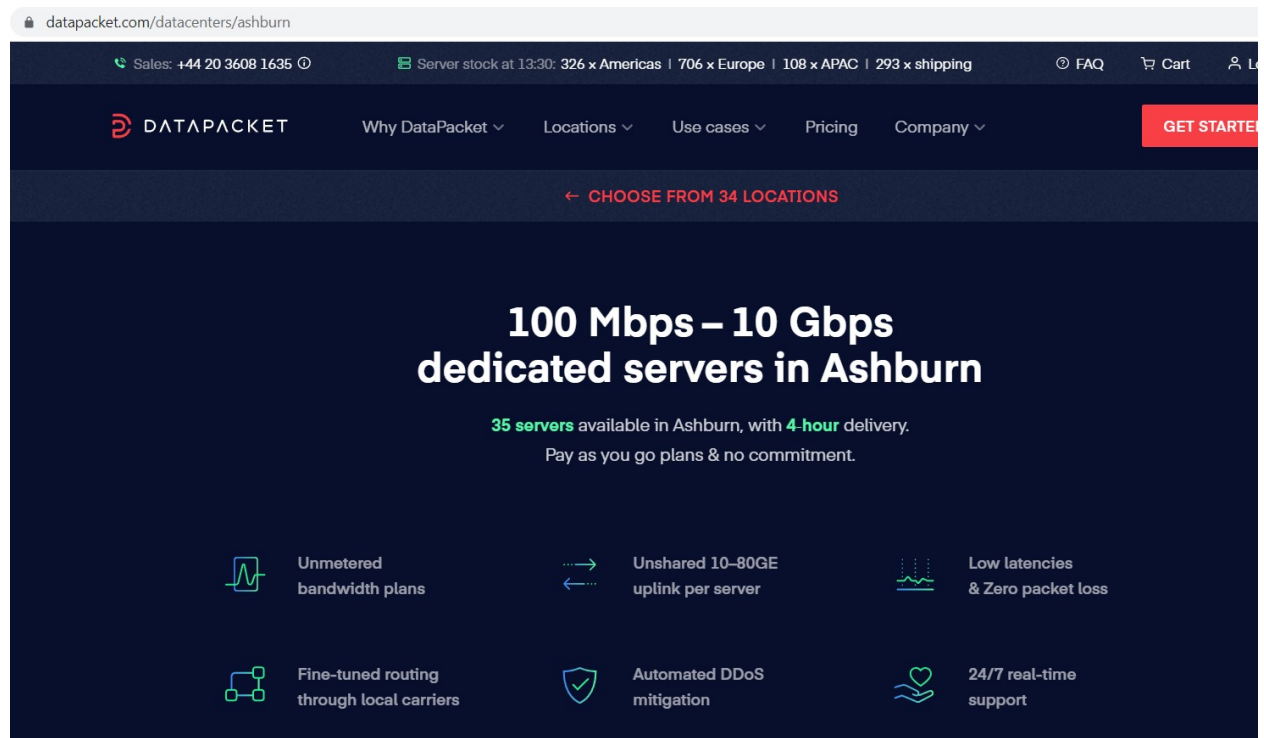
5. Defendant DataCamp operates at least thirty or more servers it leases to the public from at least one data center in Ashburn, Virginia.

6. DOES 1-10 are individuals, partnerships, corporations or other fictional entities that use DataCamp’s service such as its servers in Virginia to engage in widespread piracy of Plaintiffs’ copyright protected motion pictures.

7. In the alternative, the Court has jurisdiction over DataCamp pursuant to Fed. R. Civ. P. 4(k)(2), the so-called federal long-arm statute, for at least the following reasons: (1) Plaintiffs' claims arise under federal law; (2) DataCamp purposely directs its activity into the United States and targets and attracts a substantial number of users in the United States and, more particularly, this District; (3) DataCamp has the manifest intent of engaging in business or other interactions with the United States; (4) DataCamp not subject to jurisdiction in any state's courts of general jurisdiction; and (5) exercising jurisdiction is consistent with the United States Constitution and laws.

8. DataCamp uses many United States ("US") based sources for operating its services. DataCamp operates datacenters throughout the US under various names such as CDN77 and DataPacket including in Ashburn, Atlanta, Chicago, Dallas, Denver and Los Angeles.

9. DataCamp prominently promotes the availability of servers in the US.



10. Upon information and belief, DataCamp agreed to be subject to jurisdiction in the

US and to a Court in the US (such as Virginia or California) when agreeing to terms of services with larger host providers/data centers such as Equinix in Ashburn, Virginia and QuadraNet in Los Angeles, California to operate its service.

11. DataCamp uses US companies such as Google to promote its services to US consumers.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) - (c) because: (a) all or a substantial part of the events or omissions giving rise to the claims occurred in this District; and/or (c) Defendants are subject to the court's personal jurisdiction with respect to the present action. Additionally, venue is proper in this District pursuant 28 U.S.C. § 1400(a) (venue for copyright cases), because the Defendants or Defendants' agents resides and/or can be found in this District.

III. PARTIES

A. The Plaintiffs

13. The Plaintiffs are owners of the copyrights for the motion pictures (hereafter: "Works"), respectively, as shown in Exhibit "1".

14. Plaintiff VOLTAGE HOLDINGS, LLC is a Nevada limited liability company with its principal place of business at 116 N. Robertson Blvd, Suite 200, Los Angeles, CA 90048.

15. Plaintiff MILLENNIUM FUNDING, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

16. Plaintiff SCREEN MEDIA VENTURES, LLC is a Delaware limited liability company with its principal place of business at 800 Third Ave., 3rd Floor, New York, NY 10022.

17. Plaintiff DALLAS BUYERS CLUB, LLC is a Texas limited liability company with its principal place of business at 7 Switchbud Pl, Ste 192, The Woodlands, TX 77380.

18. Plaintiff WONDER ONE, LLC is a Wyoming limited liability company with its principal place of business at 4164 Weslin Ave. Sherman Oaks, CA 91423.

19. Plaintiff MILLENNIUM IP, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

20. Plaintiff I AM WRATH PRODUCTIONS, INC. is a California corporation with its principal place of business at 1901 Ave of the Stars Suite 1050, Los Angeles, CA 90067.

21. Plaintiff AMBI DISTRIBUTION CORP. is a Delaware corporation with its principal place of business at 3415 S. Sepulveda Blvd., 11th Fl. Los Angeles, California 90034.

22. Plaintiff KILLING LINK DISTRIBUTION, LLC is a California limited liability company with its principal place of business at 9190 Olympic Blvd. Suite 400, Beverly Hills, CA 90212.

23. Plaintiff BADHOUSE STUDIOS, LLC is a Wyoming limited liability company with its principal place of business at 8265 Sunset Blvd., Suite 107, West Hollywood, CA 90046.

24. Plaintiff LF2 PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

25. Plaintiff LHF PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

26. Plaintiff LAUNDRY FILMS, INC. is a California corporation with its principal place of business in Venice, California.

27. Plaintiff VENICE PI, LLC is a California limited liability company with its principal place of business at 116 N Robertson Blvd Ste #200, Los Angeles, CA 90048.

28. Plaintiff RAMBO V PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

29. Plaintiff SPEED KILLS PRODUCTIONS, INC. is a Wyoming corporation with its principal place of business at 8265 Sunset Blvd., Suite 107 West Hollywood, CA 90046.

30. Plaintiff NIKOLA PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

31. Plaintiff BODYGUARD PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

32. Plaintiff OUTPOST PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

33. Plaintiff AFTER II MOVIE, LLC is a Nevada limited liability company with its principal place of business at Las Vegas, NV.

34. Plaintiffs are producers of popular motion pictures currently available for sale in online and brick and mortar retail stores. Many of these critically acclaimed motion pictures were released in theaters throughout the world and feature A-list actors such as Matthew McConaughey, Samuel Jackson, Ryan Reynolds, Sylvester Stallone, Nicholas Cage, and Angela Basset, among others.

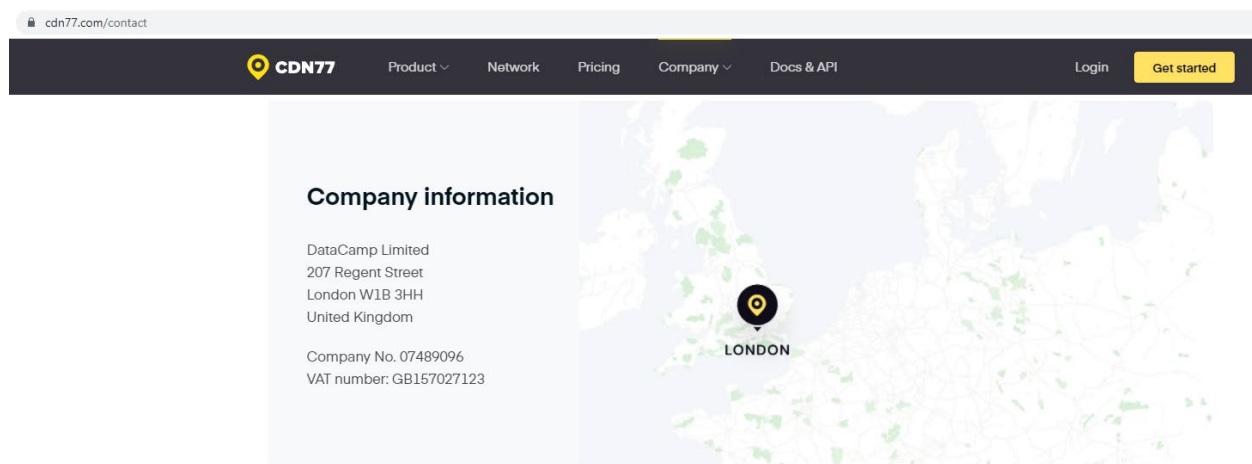
35. Plaintiffs invested significant financial resources, time and effort in making and marketing these motion pictures based upon the expectation that they would have an opportunity to get a return on their investment from rentals and sales. Massive piracy of these motion pictures by subscribers of Defendant DataCamp such as DOES 1-10 and the willful failure of DataCamp to deal with this issue despite clear notice of it have hindered this opportunity.

B. The Defendants

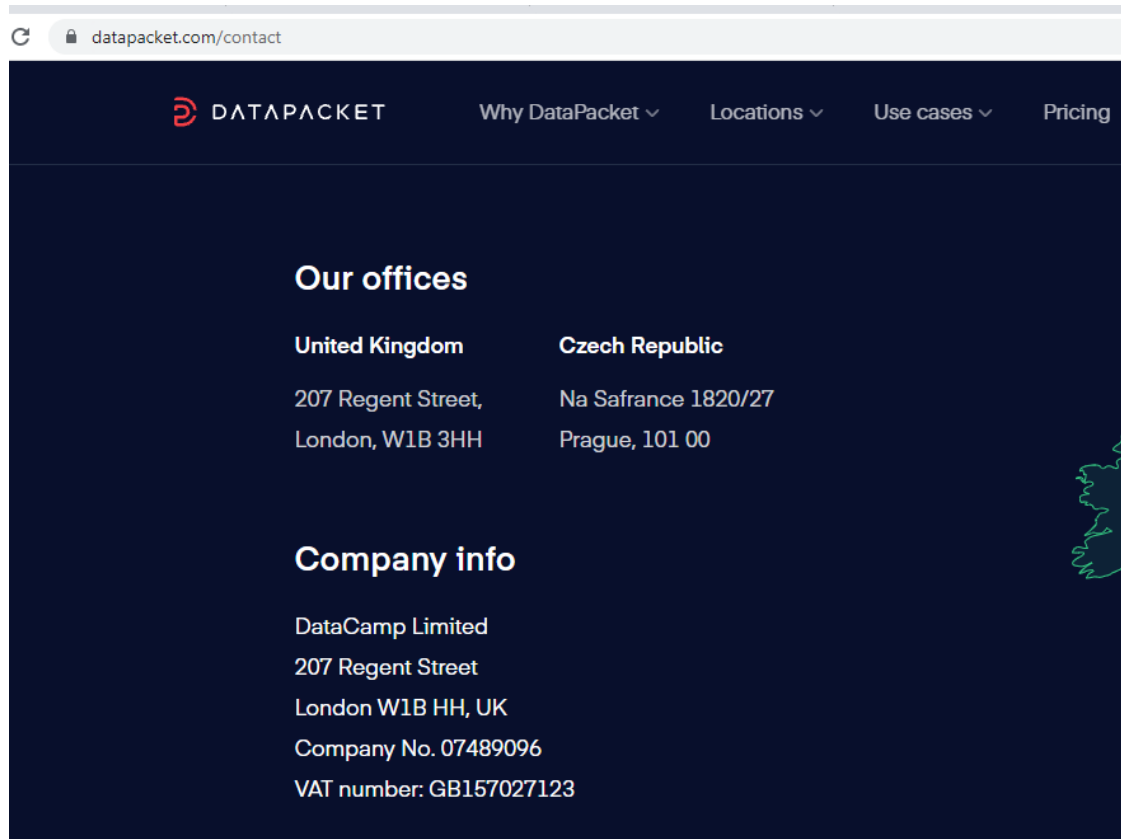
36. Defendant Datacamp is a limited company organized under the laws of the United Kingdom, and, upon information and belief, has a principal place of operations at 207 Regent Street in London W1B 3HH.

37. Upon information and belief, Datacamp does business sometimes under the names “cdn77” and “Datapacket”.

38. On the website for cdn77, it states that its company information is DataCamp Limited and gives same address as DataCamp.



39. On the website for Datapacket, it states that its company information is DataCamp Limited and gives same address as DataCamp



40. DataCamp describes itself as “operates high-performance CDN, provides high-bandwidth dedicated servers, and runs advanced network monitoring software” and “operates a global network spanning over six continents. The network topology combines upstreams to the top 14 transit providers and direct access to 3000+ local networks”.

41. Upon information and belief, DataCamp maintains one or more membership handles with the American Registry of Internet Numbers (“ARIN”) and/or the Réseaux IP Européens Network Coordination Centre (RIPE)

42. DataCamp’s ARIN and/or RIPE handles include “CDN77_DAL-EQ6”.

43. DataCamp is required to update the WHOIS records for the IP addresses it reassigns or reallocates to its subscribers per its agreement with ARIN and/or RIPE.

44. DOES 1-10 are subscribers of DataCamp.

45. DOES 1-10 provide Virtual Private Network (“VPN”) services to their own subscribers referred to here as “end users” to distinguish from DataCamp’s subscribers.

46. A VPN is a type of Internet Service that provides access to the Internet. A conventional ISP will assign its subscriber an IP address and log the subscriber’s activities on the Internet while using the assigned IP address. In comparison, many VPN providers provide their subscribers “anonymous” usage by, for example, not logging subscriber access, assigning the subscriber IP addresses that are simultaneously shared among many users, and/or encrypting traffic.

47. DOE 1-10 promote their VPN service as a tool that can be used to pirate copyright protected content without getting caught.

48. DOE 1-10 partner with notorious movie piracy websites to promote their VPN service as an essential tool for movie piracy.

49. Plaintiffs are informed and believe that Defendant is in possession of identification information or information that will lead to the identities of DOES 1-10 such as payment information. However, further discovery may be necessary in some circumstances in order to be certain of the identity of the proper Defendant. Plaintiffs believe that information obtained in discovery will lead to the identification of each of Defendants DOES 1-10’s true names and permit the Plaintiffs to amend this Complaint to state the same. Plaintiffs further believe that the information obtained in discovery may lead to the identification of additional infringing parties to be added to this Complaint as defendants. Plaintiffs will amend this Complaint to include the proper names and capacities when they have been determined. Plaintiffs are informed and believe, and based thereon allege, that each of the fictitiously named Defendants participated in and are responsible for the acts described in this Complaint and damages resulting therefrom.

C. Non-parties

50. ARIN is a nonprofit, member-based organization that manages and distributes Internet number resources such as IP addresses and Autonomous System Numbers (ASNs).

51. Members of ARIN such as Defendant are required to agree to terms of a registration agreement.

52. RIPE is the regional Internet registry that manages and distributes Internet number resources such as IP addresses for Europe, West Asia, and the former USSR.

53. Members of RIPE such as Defendant are required to agree to terms of a registration agreement.

IV. JOINDER

54. Pursuant to Fed. R. Civ. P. 20(a)(1), each of the Plaintiffs are properly joined because, as set forth in detail above and below, the Plaintiffs assert: (a) a right to relief arising out of the same transaction, occurrence, or series of transactions, namely Defendant DataCamp provides the Internet services that Defendants DOES 1-10 uses to directly infringe Plaintiffs' copyright protected Works; and (b) that there are common questions of law and fact.

V. FACTUAL BACKGROUND

A. The Plaintiffs Own the Copyrights to the Works

55. The Plaintiffs are the owners of the copyright in the Works, respectively. The Works are the subjects of copyright registrations, and this action is brought pursuant to 17 U.S.C. § 411. *See* Exhibit "1".

56. Each of the Works are motion pictures currently offered for sale in commerce.

57. Defendants had notice of Plaintiffs' rights through at least the credits indicated in the content of the motion pictures which bore proper copyright notices.

58. Defendants also had notice of Plaintiffs' rights through general publication and advertising associated with the motion pictures, and packaging and copies, each of which bore a proper copyright notice.

59. Defendant DataCamp also had notice of Plaintiffs' rights through notices Plaintiffs' agent sent to DataCamp's abuse contact as discussed below. *See* Exhibit "3".

B. Defendant DataCamp's subscribers infringe Plaintiffs' Copyrights

60. Upon information and belief, Defendant DataCamp's subscribers (DOES 1-10) include VPN providers.

61. Customers of Defendants DOES 1-10 ("end users") use BitTorrent to infringe Plaintiffs' exclusive rights of reproduction, performance and distribution.

62. The end users use the service of DataCamp's subscribers to stream or distribute copies of Plaintiffs' Works in violation of geographic regional restrictions

63. Defendant DataCamp's subscribers distribute Plaintiffs' Works for these end users in violation of Plaintiffs' exclusive right of distribution.

64. Defendant DataCamp's subscribers reproduce Plaintiffs' Works for these end users in violation of Plaintiffs' exclusive right of distribution.

65. Defendant DataCamp's subscribers stream Plaintiffs' Works for these end users in violation of Plaintiffs' exclusive right of public performance.

1. End Users installed a BitTorrent Client onto his or her Computer

66. BitTorrent is one of the most common peer-to-peer file sharing protocols (in other words, set of computer rules) used for distributing large amounts of data.

67. The BitTorrent protocol's popularity stems from its ability to distribute a large file without creating a heavy load on the source computer and network. In short, to reduce the load on

the source computer, rather than downloading a file from a single source computer (one computer directly connected to another), the BitTorrent protocol allows users to join a “swarm” of host computers to download and upload from each other simultaneously (one computer connected to numerous computers).

68. A BitTorrent Client is a software program that implements the BitTorrent Protocol. There are numerous such software programs which can be directly downloaded from the Internet.

69. Once installed on a computer, the BitTorrent Client serves as the user’s interface during the process of uploading and downloading data using the BitTorrent protocol.

70. A BitTorrent user that wants to upload the new file, known as an “initial seeder,” starts by creating a “torrent” descriptor file using, for example, the Client he or she installed onto his or her computer.

71. The initial user or seeder of a file used a process referred to as “ripping” to create a copy of motion pictures from either Blu-ray or legal streaming services.

72. The initial seeder often modifies the file title of the Work to include a wording such as “FGT”, “RARBG” or “YTS” in the title of the torrent files and file copies in order to enhance a reputation for the quality of his or her torrent files and attract users to his or her piracy website.

73. The Client takes the target computer file, the “initial seed,” here the copyrighted Work, and divides it into identically sized groups of bits known as “pieces.”

74. The Client then gives each one of the computer file’s pieces, in this case, pieces of the copyrighted Works, a random and unique alphanumeric identifier known as a “hash” and records these hash identifiers in the torrent file.

75. When another peer later receives a particular piece, the hash identifier for that piece is compared to the hash identifier recorded in the torrent file for that piece to test that the piece is

error-free. In this way, the hash identifier works like an electronic fingerprint to identify the source and origin of the piece and that the piece is authentic and uncorrupted.

76. Torrent files also have an "announce" section, which specifies the URL (Uniform Resource Locator) of a "tracker," and an "info" section, containing (suggested) names for the files, their lengths, the piece length used, and the hash identifier for each piece, all of which are used by Clients on peer computers to verify the integrity of the data they receive.

77. The "tracker" is a computer or set of computers that a torrent file specifies and to which the torrent file provides peers with the URL address(es).

78. The tracker computer or computers direct a peer user's computer to other peer user's computers that have particular pieces of the file, here the copyrighted Work, on them and facilitates the exchange of data among the computers.

79. Depending on the BitTorrent Client, a tracker can either be a dedicated computer (centralized tracking) or each peer can act as a tracker (decentralized tracking.)

2. Torrent Sites

80. "Torrent sites" are websites that index torrent files that are currently being made available for copying and distribution by people using the BitTorrent protocol. There are numerous torrent websites including the notorious Pirate Bay, YTS and RARBG websites.

81. The Pirate Bay, YTS and RARBG websites were noted by the USTR as examples of Notorious Markets defined as an online marketplace reportedly engaged in and facilitating substantial piracy. *See* USTR, 2014 Out-of-Cycle Review of Notorious Markets, Mar. 5, 2015, pg. 17, Available at https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published_0.pdf [last accessed on May 7, 2021]; USTR, *2018 Out-of-Cycle Review of*

Notorious Markets, April 2019, pgs. 24, 27-28 Available at https://ustr.gov/sites/default/files/2018_Notorious_Markets_List.pdf [accessed on May 7, 2021].

82. Once the initial seeder has created a torrent and uploaded it onto one or more torrent sites, then other peers begin to download and upload the computer file to which the torrent is linked (here the copyrighted Work) using the BitTorrent protocol and BitTorrent Client that the peers installed on their computers.

83. The BitTorrent protocol causes the initial seeder's computer to send different pieces of the computer file, here the copyrighted Work, to the peers seeking to download the computer file. End users use DataCamp's servers in the United States to transmit the pieces to the peers.

84. Once a peer receives a piece of the computer file, here a piece of the copyrighted Work, it starts transmitting that piece to the other peers. Defendants' subscribers (DOES 1-10) transmit the pieces to the peers.

85. In this way, all of the peers and seeders are working together in what is called a "swarm."

3. The Plaintiffs' Computer Investigator Identified DataCamp's IP Addresses as Participants in Swarms That Were Distributing Plaintiffs' Copyrighted Works.

86. The Plaintiffs retained Maverickeye UG ("MEU") to identify the IP addresses that are being used by those people that are using the BitTorrent protocol and the Internet to reproduce, distribute, display or perform the Plaintiff's copyrighted Work.

87. MEU used forensic software to enable the scanning of peer-to-peer networks for the presence of infringing transactions.

88. MEU extracted the resulting data emanating from the investigation, reviewed the evidence logs, and isolated the transactions and the IP addresses associated therewith for the files identified by the SHA-1 hash value of the Unique Hash Number.

89. The logged information show that DataCamp's subscribers (including but not limited to DOES 1-10) distributed pieces of the Plaintiffs' copyrighted Works identified by the Unique Hash Number.

90. End users' computers used the identified IP addresses such as Internet Protocol ("IP") address 89.187.164.179 to connect to the investigative server from a computer in this District in order to transmit a full copy, or a portion thereof, of a digital media file identified by the Unique Hash Number.

91. MEU's agent analyzed each BitTorrent "piece" distributed by the IP addresses and verified that re-assemblage of the pieces using a BitTorrent Client results in a fully playable digital motion picture of the Works.

92. MEU's agent viewed the Works side-by-side with the digital media file that correlates to the Unique Hash Number and determined that they were identical, strikingly similar or substantially similar.

C. The Operator of the YTS website confirmed that the end users downloaded torrent files for copying the Work from the YTS website.

93. The YTS website operator maintained records of activity of registered user accounts. See Exhibit "2" at pg. 71 (Certificate of Authenticity).

94. As shown in Exhibit "2", the records include the email address of the registered user account, the torrent files the registered account downloaded, the IP address from where the registered user accessed the YTS website, and the time.

95. The records show end users downloaded the torrent files for reproducing Plaintiffs' motion pictures from IP addresses assigned to Defendant DataCamp and in, some cases, in Ashburn Virginia.

96. Some of these YTS users the VPN service of DataCamp's subscribers to unlawfully access "hack" into the accounts of third parties, use their email addresses to register for an account with the YTS website and pirate movies, and unlawfully access bank accounts of the third parties. *See Decl. of Daniel W. Byanski.*

D. Defendant DataCamp's subscribers distributed copies of Plaintiffs' Works with altered CMI.

97. Defendant DataCamp's subscribers distributed at least pieces of each of Plaintiffs' Works over network connections to other peers in the Swarm from IP addresses allocated from DataCamp with file names that included modified copyright management information ("CMI").

98. DataCamp allocated or reassigned IP addresses 89.187.164.179, 89.187.171.116, 89.187.182.111, 156.146.50.1, 156.146.50.134, 156.146.50.65, 156.146.50.198, 89.187.187.129, 156.146.47.11, 89.187.187.162 to its subscribers.

99. DataCamp's subscribers distributed copies of the motion pictures with file names altered to include CMI from these IP addresses.

100. For example, DataCamp's subscriber at IP address 89.187.164.179 distributed copies of the Work *Rambo V: Last Blood* under the file name "Rambo Last Blood (2019) [BluRay] [720p] [YTS.LT]".

F. Defendant DataCamp's subscribers (DOES 1-10) knew the CMI included in the files they distributed to other peers had been removed or altered without the authority of Plaintiffs.

101. Legitimate file copies of the Works include CMI indicating the respective title.

102. The initial seeder of the infringing file copies of Plaintiffs' Works added wording to the file titles to "brand" the quality of piracy files he or she released and attract further traffic to his or her website.

103. For example, the initial seeder of the infringing file copies of *Rambo V: Last Blood* added the wording "YTS" to the file titles to brand the quality of piracy files he or she released and attract further traffic to the YTS website.

104. The word YTS is not included in the file title of legitimate copies or streams of the Plaintiffs' Works. The initial seeders of the Work altered the title to falsely include the words "YTS" in the CMI.

105. The file copies Defendant Defendant's subscribers distributed to other peers in the Swarm included the altered CMI in the file title.

106. Defendants DOES 1-10 knew that FGT, YTS and RARBG were not the author of Plaintiffs' Works.

107. Defendants DOES 1-10 knew that FGT, YTS and RARBG were not a licensed distributor of Plaintiffs' Works. Indeed, the YTS website includes a warning to this effect.

108. Defendants DOES 1-10 knew that the CMI that included YTS and RARBG in the file names was false.

109. Defendants DOES 1-10 knew that the file copies of the Work that they distributed to other peers from in the Swarm included the altered CMI without the authority of Plaintiffs.

110. Defendants DOES 1-10 knew that the CMI in the title they distributed to other peers in the Swarm included the altered CMI without the authority of Plaintiffs.

111. Defendants DOES 1-10 knew that the false or altered CMI in the titles would induce, enable, facilitate or conceal infringements of the Works when they distributed the false CMI, altered CMI or Works including the false or altered CMI.

112. Namely, DOES 1-10 knew that other recipients would see the file titles and use the altered CMI to go to the website such as YTS from where the torrent files originated to obtain unlicensed copies of the Work.

113. By providing the website in the altered CMI to others, Defendants DOES 1-10 induced, enabled and facilitated further infringements of the Works

G. Defendant DataCamp had knowledge that its subscribers were infringing Plaintiffs' Works by distributing file copies of the Works with altered CMI but continued to provide service to its subscribers

114. Plaintiffs engaged MEU to generate Notices of infringements ("Notices") styled per 17 U.S.C. §512(c)(3) of the DMCA to be sent to service providers of IP addresses where MEU confirmed infringement of copyright protected content.

115. Each Notice included at least the name of the copyright owner, the title of the Work, the manner by which it was infringed, the infringing file name which includes the altered CMI, the IP address and port number at where infringement was confirmed and the time of infringement down to the second. *See* Exhibit "3" (excerpt below).

Protocol: BITTORRENT
Infringed Work: Rambo: Last Blood
Infringing FileName: Rambo Last Blood (2019) [BluRay] [720p] [YTS.LT] Infringing FileSize: 953581534
Infringer's IP Address: 89.187.164.179 Infringer's Port: 50406 Initial Infringement Timestamp: 2021-02-17 04:52:26

116. MEU determines the proper abuse contact email address for the service provider assigned the IP addresses at issue from publicly available information.

117. Plaintiffs' agent sends the Notice to Defendant DataCamp's abuse contact email address (abuse@cdn77.com).

118. Plaintiffs' agent has sent over 78,500 Notices to DataCamp concerning infringements of copyright protected Works including DataCamp's at IP addresses assigned to DataCamp from ARIN or RIPE.

119. Plaintiffs' agent sent over 12,300 Notices to DataCamp concerning infringement of the motion picture *Ava* at IP addresses assigned to DataCamp.

120. Plaintiffs' agent sent over 8500 Notices to DataCamp concerning infringement of the motion picture *Tesla* at IP addresses assigned to DataCamp from ARIN.

121. Plaintiffs' agent sent over 4600 Notices to DataCamp concerning infringement of the motion picture *Angel Has Fallen* at IP addresses assigned to DataCamp .

122. Plaintiffs' agent sent over 4900 Notices to DataCamp concerning infringement of the motion picture *Rambo V: Last Blood* at IP addresses assigned to DataCamp.

123. Plaintiffs' agent sent over 10,000 Notices to DataCamp concerning infringement of the motion picture *Outpost* at IP addresses assigned to DataCamp.

124. Plaintiffs' agent sent over 3000 Notices to DataCamp concerning infringement of the motion picture *Hellboy* at IP addresses assigned to DataCamp.

125. Plaintiffs' agent sent over 900 Notices to DataCamp concerning infringement of the motion picture *Kill Chain* at IP addresses assigned to DataCamp from ARIN.

126. Plaintiffs' agent sent 1400 Notices to DataCamp concerning observed infringements at IP addresses 89.187.164.179.

127. Plaintiffs' agent sent 400 Notices to DataCamp concerning observed infringements at each of IP addresses 89.187.171.116, 89.187.182.111, 156.146.50.1, 156.146.50.134,

156.146.50.65, 156.146.50.198, 89.187.187.129, 156.146.47.11, 89.187.187.162 (total of over 3600 Notices for these nine IP addresses).

128. Upon information and belief, other rightsholders had similar Notices sent to DataCamp concerning infringing activity at IP addresses assigned to Defendant.

129. DataCamp failed to terminate the subscribers such as DOES 1-10 or the accounts associated with these IP addresses or take any meaningful action in response to these Notices.

130. DataCamp failed to even forward one or more of the Notices to its subscribers such as to DOES 1-10.

131. DataCamp continued to provide service to the subscribers such as DOES 1-10 despite knowledge that its subscribers were using the service to engage and facilitate massive piracy of copyright protected Works including Plaintiffs’.

132. Even after Plaintiffs’ counsel sent a letter to DataCamp on Mar. 15, 2021 requesting DataCamp to terminate the accounts of subscribers assigned certain IP addresses where flagrant piracy had been confirmed (*see* Exhibit “3”), DataCamp completely ignored the letter and continued to provide service.

H. Defendant DataCamp controls the conduct of its subscribers.

133. Defendant DataCamp can terminate the accounts of its’ subscribers at any time.

134. Upon information and belief, DataCamp promptly suspends and terminates subscriber accounts when said subscribers failed to pay for service.

135. Upon information and belief, DataCamp monitors its subscribers’ access to its service and limits service when the subscribers consume more than a predetermined amount of bandwidth.

I. Defendant DataCamp does not have a safe harbor from liability.

136. As part of the DMCA, Congress created a safe harbor that limits the liability of a service provider for copyright infringement when their involvement is limited to, among other things, “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider.” 17 U.S.C. § 512(a). To benefit from this safe harbor, however, an ISP must demonstrate that it “has adopted and reasonably implemented...a policy that provides for the termination in appropriate circumstances of subscribers...who are repeat infringers.” 17 U.S.C. § 512(i)(1)(A).

137. Defendant DataCamp has not adopted and/or reasonably implemented a policy of terminating repeat infringers.

138. Plaintiffs’ agent has sent over 78,500 Notices to DataCamp concerning infringements at IP addresses DataCamp publishes as assigned to it.

139. DataCamp has failed to terminate the accounts and/or take any meaningful actions against its subscribers in response to these Notices consistent with a reasonably implemented policy for termination of subscribers and account holders of the service provider’s system or network who are repeat infringers necessary to support a safe harbor from liability (“policy”).

140. Congress created a safe harbor that limits the liability of a service provider for copyright infringement “...by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider” does not have the requisite knowledge, “...responds expeditiously to remove or disable access to, the material...” and has the appropriate designated agent for receiving notices. 17 U.S.C. § 512(c)(1), (2).

141. DataCamp leases use of its servers to its subscribers so that the subscribers can host VPN networks on its servers.

142. DataCamp's subscribers (DOES 1-10) store copies of Plaintiffs' Works on DataCamp's servers and use DataCamp's servers to distribute copies of Plaintiffs' Works.

143. The over 78,500 Notices Plaintiffs' agent sent to DataCamp concerning infringements included information such as the IP addresses that DataCamp could have used to remove or disable access to infringing material.

144. DataCamp failed to respond and expeditiously remove or disable access to the material in response to the over 78,500 Notices Plaintiffs' agent sent to DataCamp.

145. DataCamp failed to designate and register an agent with the Copyright Office as provided by 17 U.S.C. § 512(c)(2).

146. DataCamp's conduct renders it ineligible for safe harbor immunity from copyright liability under the DMCA.

J. The copyright infringements arise from Defendant DataCamp's advertisements.

147. Defendant DataCamp advertises high-bandwidth dedicated servers.

148. DataCamp's subscribers are motivated to become customers from Defendant's advertisements.

149. DataCamp's subscribers are motivated to become customers from the knowledge of DataCamp's practice of ignoring notices of infringements or failing to take any meaningful action in response to said notices.

**VI. FIRST CLAIM FOR RELIEF
(Direct Copyright Infringement against Defendants DOES 1-10)**

150. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

151. Plaintiffs are the copyright owners of the Works, each of which contains an original work of authorship.

152. Defendants DOES 1-10's actively promote their VPN service for piracy and encourage their customers ("end users") to use their VPN service for piracy.

153. Defendants DOES 1-10 transmit, route, or provide connections for transmitting copies of Plaintiffs' Works through a network under their control including servers provided by DataCamp.

154. Defendants DOES 1-10 distributed and made copies of copyright protected Works to others on said network when transmitting, routing, or providing connections for transmitting copies of Plaintiffs' Works through said network.

155. Defendants DOES 1-10 encourage their end users to use the network to distribute and reproduce copies of Plaintiffs' Works.

156. Defendants DOES 1-10 distributed, perform and reproduced the constituent elements of Plaintiffs' copyright protected Works via networks under their control without authorization in violation of the Plaintiffs' exclusive right to reproduce, perform and distribute the Works in copies, in violation of 17 U.S.C. §§ 106(1), 106(3), 106(4) and 501.

157. Defendants DOES 1-10 interfere with standard technical measures used by copyright holders to identify or protect copyright works by purposefully deleting their end users' log information. *See* 17 U.S.C. § 512(i)(1)(B).

158. DOES 1-10 connect the end users to torrent sources to provide said at least a piece.

159. DOES 1-10 distribute said at least a piece for Defendants DOES 11-100 with knowledge that said at least a piece infringes Plaintiffs' rights.

160. Defendants DOES 1-10's infringements were committed "willfully" within the meaning of 17 U.S.C. § 504(c)(2).

161. Plaintiffs have suffered damages that were proximately caused by the Defendants DOES 1-10's copyright infringements including, but not limited to lost sales, price erosion, and a diminution of the value of its copyright.

VII. SECOND CLAIM FOR RELIEF
(Contributory Copyright Infringement based upon material contribution against
DataCamp and DOES 1-10)

162. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

163. Through its activities, Defendants DataCamp and DOES 1-10 knowingly and intentionally took steps that are substantially certain to result in direct infringement of Plaintiffs' Copyrighted Works, and that have resulted in such direct infringement in violation of Plaintiffs' copyrights.

164. Despite Defendant DataCamp's knowledge that its subscribers such as DOES 1-10 are using its service to engage in widescale copyright infringements, Defendant DataCamp has failed to take reasonable steps to minimize the infringing capabilities of its service.

165. Defendant DataCamp is liable as contributory copyright infringers for the infringing acts of its subscribers such as DOES 1-10. Defendant DataCamp has actual and constructive knowledge of the infringing activity of its subscribers. Defendant DataCamp knowingly caused and otherwise materially contributed to these unauthorized distributions of Plaintiffs' Works.

166. Despite Defendants DOES 1-10's knowledge that end users are using its service to engage in widescale copyright infringements, DOES 1-10 have failed to take reasonable steps to minimize the infringing capabilities of its service.

167. Defendants DOES 1-10 are liable as contributory copyright infringers for the infringing acts of their end users. Defendants DOES 1-10 have actual and constructive knowledge

of the infringing activity of their end users. Defendant DOES 1-10 knowingly caused, encouraged and otherwise materially contributed to these unauthorized distributions of Plaintiffs' Works.

168. Defendants DataCamp and DOES 1-10's infringements were committed "willfully" within the meaning of 17 U.S.C. § 504(c)(2).

169. By engaging in the contributory infringement alleged in this Complaint, Defendants DataCamp and DOES 1-10 deprived not only the producers of the Works from income that could have been derived when the respective film was shown in public theaters and offered for sale or rental, but also all persons involved in the production and marketing of this film, numerous owners of local theaters and retail outlets and their employees, and, ultimately, the local economy. Defendants' misconduct therefore offends public policy.

VIII. THIRD CLAIM FOR RELIEF (Vicarious Infringement against DataCamp and DOES 1-10)

170. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

171. Defendant DataCamp is vicariously liable for the infringing acts of its subscribers' infringements including but not limited to the subscribers' direct infringements of Plaintiffs' exclusive right to distribute copies of their Works.

172. Defendants DOES 1-10 are vicariously liable for the infringing acts of their end users including but not limited to the end users' direct infringements of Plaintiffs' exclusive right to distribute and reproduce copies of their Works.

173. Defendant DataCamp has the right and ability to supervise and control the infringing activities that occur through the use of its service, and at all relevant times has derived a direct financial benefit from the infringement of Plaintiffs' copyrights.

174. Defendant DataCamp has refused to take any meaningful action to prevent the widespread infringement by its subscribers such as DOES 1-10 despite having actual knowledge. Indeed, the ability of subscribers such as DOES 1-10 to use Defendant DataCamp's high bandwidth dedicated servers to distribute copies of Plaintiffs' Works for end users serves as a powerful draw for users of Defendant DataCamp's service.

175. Defendants DOES 1-10 have the right and ability to supervise and control the infringing activities that occur through the use of its service, and at all relevant times has derived a direct financial benefit from the infringements of Plaintiffs' copyrights.

176. Defendants DOES 1-10 have refused to take any meaningful action to prevent the widespread infringement by its end users despite having actual knowledge. Indeed, the ability of the end users to use Defendants DOES 1-10's service to distribute copies of Plaintiffs' Works while concealing their identities acts as a powerful draw for users of Defendants DOES 1-10's service.

177. Defendants DataCamp and DOES 1-10 could take simple measures such as null-routing IP addresses to stop unauthorized distribution of Plaintiffs' Works over servers controlled by them but purposefully refuse to do so.

178. Defendants DOES 1-10 could take simple measures such as logging their end users' access to servers controlled by them that they lease from DataCamp to identify end users engaged in unauthorized distribution of Plaintiffs' Works and stop said end users from engaging in infringement but purposefully refuse to do so.

179. Indeed, the ability of subscribers such as Defendants DOES 1-10 to use DataCamp's service to host and operate their VPN service to distribute, stream and reproduce copies of Plaintiffs' Works while concealing their end users' identities acts as a powerful draw for users of DataCamp's service.

180. DataCamp's subscribers are also motivated to become subscribers of DataCamp due to their knowledge that they can pirate Plaintiffs' Works without any consequence because of DataCamp's policy of failing to take meaningful action in response to notices of infringement.

181. DataCamp's subscribers are also motivated to become subscribers of DataCamp due to their knowledge of DataCamp's policy of failing to update the ARIN or RIPE Whois records so that copyright owners could not send notices of infringements to them and thereby pirate Plaintiffs' Works without any consequence.

182. DataCamp directly benefits from its subscribers' piracy of Plaintiffs Works. As the subscribers attract more end users that wish to use the VPN service to pirate Plaintiffs' Works, DataCamp's subscribers purchase more server space, IP addresses, and/or colocations services.

183. Defendants DataCamp and DOES 1-10 are therefore vicariously liable for the unauthorized distribution of Plaintiffs' Works.

VIII. FOURTH CLAIM FOR RELIEF
(Secondary Liability for Digital Millennium Copyright Act Violations)

184. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

185. Defendant DataCamp's subscribers such as DOES 1-10 encourage their end users to access torrent files for copying copyright protected Works from notorious movie piracy websites such as YTS.

186. Defendant DataCamp's subscribers such as Defendants DOES 1-10, and their end users knowingly and with the intent to induce, enable, facilitate, or conceal infringement of the Plaintiffs' copyright protected Works, distributed copyright management information ("CMI")

that falsely included false wording such as “RARBG”, “FGT” and “YTS” in violation of 17 U.S.C. § 1202(a)(2).

187. Defendant DataCamp’s subscribers such as Defendants DOES 1-10, and their end users, without the authority of Plaintiffs, or the law, distributed removed or altered CMI knowing that the CMI had been removed or altered to include the wording “RARBG”, “FGT” and “YTS” without the authority of Plaintiffs and knowing, or having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement of Plaintiffs’ copyright protected Works in violation of 17 U.S.C. § 1202(b)(2).

188. Defendant DataCamp’s subscribers such as Defendants DOES 1-10, and their end users, without the authority of Plaintiffs, or the law, distributed Plaintiffs’ Copyright protected Works knowing that the CMI had been removed or altered to include the wording RARBG”, “FGT” or “YTS”, and knowing, or having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement of the copyright protected Works in violation of 17 U.S.C. § 1202(b)(3).

189. Particularly, Defendant DataCamp’s subscribers such as Defendants DOES 1-10, and their end users knew that the CMI in the file names of the pieces had been altered to include the wording “RARBG”, “FGT” or “YTS”.

190. Particularly, Defendant DataCamp’s subscribers such as Defendants DOES 1-10, and their end users distributed the file names that included CMI that had been altered to include the wording “RARBG”, “FGT” or “YTS”.

191. Defendant DataCamp’s subscribers such as Defendants DOES 1-10, and their end users knew that the wording “RARBG”, “FGT” or “YTS” originated from notorious movie piracy websites which they themselves promoted.

192. Defendant DataCamp's subscribers such as Defendants DOES 1-10, and their end users' acts constitute violations under the Digital Millennium Copyright Act, 17 U.S.C. § 1202.

193. Defendants DataCamp and DOES 1-10 are secondarily liable for the DMCA violations of their subscribers and end users. Defendants DataCamp and DOES 1-10 had actual and constructive knowledge of their subscribers' and end users' DMCA violations. Defendants DataCamp and DOES 1-10 knowingly caused and otherwise materially contributed to these DMCA violations.

194. Defendants DataCamp and DOES 1-10 are vicariously liable for the DMCA violations of their subscribers and end users. Defendants DataCamp and DOES 1-10 have the right and ability to supervise and control the DMCA violations that occur through the use of their service, and at all relevant times has derived a direct financial benefit from the DMCA violations complained of herein.

195. Defendant DataCamp has refused to take any meaningful action to prevent the widespread DMCA violations by its subscribers. Indeed, the ability of Defendant DataCamp's subscribers to distribute torrent files from torrent websites such as YTS that DataCamp's subscribers themselves promote and obtain file copies of the Works with altered CMI and distribute said copies while concealing their end users' activities acts as a powerful draw for subscribers of Defendant DataCamp. Defendant DataCamp is therefore vicariously liable for its subscribers' DMCA violations.

196. Defendants DOES 1-10 have has refused to take any meaningful action to prevent the widespread DMCA violations by their end users. Indeed, the ability of Defendants DOES 1-10's end users to distribute torrent files from using BitTorrent Clients such as Popcorn Time that DOES 1-10 themselves promote and obtain file copies of the Works with altered CMI and

distribute said copies while concealing their end users' activities acts as a powerful draw for subscribers of Defendants DOES 1-10. Defendants DOES 1-10 are therefore vicariously liable for their end users' DMCA violations.

197. Plaintiffs are entitled to an injunction to prevent Defendants from engaging in further violations of 17 U.S.C. § 1202.

198. Plaintiffs are entitled to recover from Defendants the actual damages suffered by Plaintiffs and any profits Defendants have obtained as a result of its wrongful acts that are not taken into account in computing the actual damages. Plaintiffs are currently unable to ascertain the full extent of the profits Defendant has realized by its violations of 17 U.S.C. § 1202.

199. Plaintiffs are entitled to elect to recover from Defendants statutory damages for its violations of 17 U.S.C. § 1202.

200. Plaintiffs are further entitled to costs and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs respectfully request that this Court:

(A) enter permanent injunctions enjoining Defendants from continuing to commit DMCA violations, and infringe and contribute to infringements of the Plaintiffs' copyrighted Works;

(B) order Defendants to adopt a policy that provides for the prompt termination of subscribers and end users that engage in more than three infringements of copyright protected Works;

(C) order Defendants to block ports 6881-6889 on all of the servers under their control to prevent further pirating of Plaintiffs' Works via the BitTorrent protocol;

(D) order Defendants and all service providers that received notice of this order pursuant to 17 U.S.C. §§ 512(j)(1)(A) and (B) to block subscribers from accessing notorious piracy websites

of foreign origin that are listed in the annual trade report of Notorious Foreign Markets published by the United States Government such as (a) YTS; (b) Piratebay; (c) Rarbg; (d) 1337x; and (e) PopcornTime on networks under their control

(E) award the Plaintiffs their actual damages from the copyright infringements and Defendants' profits in such amount as may be found; alternatively, at Plaintiffs' election, for statutory damages pursuant to 17 U.S.C. § 504(a) and (c) against Defendants;

(F) award the Plaintiffs actual damages from the DMCA violations and Defendants' profits in such amount as may be found; or, in the alternative, at Plaintiffs' election, for statutory damages per DMCA violation pursuant to 17 U.S.C. § 1203(c) for violations of 17 U.S.C. § 1202 against Defendants;

(G) award the Plaintiffs their reasonable attorneys' fees and costs pursuant to 17 U.S.C. § 505 and/or 17 U.S.C. § 1203(b)(5); and

(H) grant the Plaintiffs any and all other and further relief that this Court deems just and proper.

The Plaintiffs hereby demand a trial by jury on all issues properly triable by jury.

DATED: Kailua Kona, HI, September 30, 2021.

Respectfully submitted,

/s/ Kerry S. Culpepper

Kerry S. Culpepper,
Virginia Bar No. 45292
Counsel for Plaintiffs
CULPEPPER IP, LLC
75-170 Hualalai Road, Suite B204
Kailua-Kona, Hawai'i 96740
Tel.: (808) 464-4047
Fax.: (202) 204-5181
kculpepper@culpepperip.com